AFRL-IF-RS-TR-2005-347
Final Technical Report
October 2005

COALITION INFORMATION ASSURANCE – COMMON OPERATING PICTURE (CIA-COP)

Northrop Grumman

AIR FORCE RESEARCH LABORATORY
INFORMATION DIRECTORATE
ROME RESEARCH SITE
ROME, NEW YORK

STINFO FINAL REPORT

This report has been reviewed by the Air Force Research Laboratory, Information Directorate, Public Affairs Office (IFOIPA) and is releasable to the National Technical Information Service (NTIS). At NTIS it will be releasable to the general public, including foreign nations.

AFRL-IF-RS-TR-2005-347 has been reviewed and is approved for publication.

APPROVED: /s/

BRIAN T. SPINK
Project Engineer

FOR THE DIRECTOR: /s/

WARREN H. DEBANY, JR., Technical Advisor
Information Grid Division
Information Directorate

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	OCTOBER 2005	Final Apr 03 – Apr 04

4. TITLE AND SUBTITLE
COALITION INFORMATION ASSURANCE – COMMON OPERATING PICTURE (CIA-COP)

5. FUNDING NUMBERS
C - F30602-99-D-0001/0019
PE - 33140F
PR - AIDE
TA - JM
WU - 19

6. AUTHOR(S)
Louis Scheiderich

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Northrop Grumman
7275 Colshire Drive
McLean Virginia 22162-7508

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory/IFGA
525 Brooks Road
Rome New York 13441-4505

10. SPONSORING / MONITORING AGENCY REPORT NUMBER
AFRL-IF-RS-TR-2005-347

11. SUPPLEMENTARY NOTES

AFRL Project Engineer: Brian T. Spink/IFGA/(315) 330-7596/ Brian.Spink@rl.af.mil

12a. DISTRIBUTION / AVAILABILITY STATEMENT
APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(Maximum 200 Words)***

This technical report summarizes and describes an effort under the subcontract task. It describes capability enhancements to the IPIB prototype decision support system, feasibility analyses, demonstration and technology transition efforts undertaken as efforts under this task.

14. SUBJECT TERMS
CAULDRON, Computer Network Operations, CON

15. NUMBER OF PAGES
11

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

Table of Contents

1.0 Purpose.

This is Zel Technologies, LLC's (ZelTech) Final Technical Report (FTR) for Intelligence Preparation of the Information Battlespace (IPIB) for Effects-based Operations (IPIB4EBO), Task 19 of AFRL Contract F30602-99-D-0001, Defensive Information Warfare Technology Applications (DIWTA). The effort was awarded to ZelTech through Northrop Grumman (NG) subcontract D022900-2000 as Task 19. The contract was managed through the Defensive Information Warfare Branch (IFGB) of the Air Force Research Lab (AFRL) in Rome, New York. The Principal Investigator (PI) was Dr. James K. Williams, Chief Technology Officer, Zel Technologies, LLC.

2.0 Background.

Program Background. Task 19 is a continuation of the Intelligence Preparation of Information Battlespace (IPIB) research initially begun in 1998 under the DARPA Cyber Panel Project, a part of the DARPA Information Assurance and Survivability project. Cyber Panel sought to provide high-level capabilities to help defend mission-critical information systems by monitoring them for signs of cyber attack and allowing operators to manage the operation of system security/survivability technologies to avert or resist attack. This program was intended to deliver technologies that could be used to build such a monitoring and management system. The goal was to create and validate architectures, algorithms, techniques, and automated tools that aid identification of coordinated attacks, assessment of system health, mission impact assessment, course of action selection, and help carry out effective security and survivability posture changes, either proactively or in response to the appearance of attacks. As the DARPA program expired in 2002, AFRL/IFGB continued funding under contract F30602-99-C-0168, the original DARPA contract, because of the initial success and potential of IPIB for enhancing network security and possible application to Computer Network Attack (CNA). In FY 2004, AFRL opted to further continue funding under the subject subcontract.

Outside the scope of the IPIB R&D effort, ZelTech was contracted by General Dynamics Corp (GD) to transition a subset of IPIB technology into the Information Warfare Planning Capability (IWPC). This subset mainly addressed *Step 2 – Define Battlespace Effects* of the IPB cycle, and was renamed the Computer Network Operations Analysis Tool (CNOAT). It required extraction and increased functionality of certain components of IPIB. However, this made IPIB one of the only IA&S projects from DARPA to successfully transition to an operational, fielded system. This also meant that for the IPIB effort itself, there was a divergent baseline – CNOAT with Defensive Information Warfare (DIW) extensions and several important IPIB capabilities removed, and the IPIB

prototype that had functionality not used in CNOAT, but did not have the CNOAT extensions. Therefore, the technical baseline for commencing Task 19 consisted of the IPIB prototype and the CNOAT DIW tool.

This technical report summarizes and describes effort under the subcontract task. It describes capability enhancements to the IPIB prototype decision support system, feasibility analyses, demonstrations and technology transition efforts undertaken as efforts under this task.

2.1 IPIB Description.

In conducting military operations in the physical world, the US Intelligence Community has developed, refined and applied a number of time-tested intelligence analysis processes and tools that provide critical support to operations and help ensure victory. Key among these processes is the Army's classic Intelligence Preparation of the Battlefield (IPB), which is documented in Army Field Manual (FM) 34-130. IPB provides the analyst a structured methodology and a set of tools to perform predictive intelligence for land warfare by analyzing the mission, enemy, terrain, available time, weather and other significant factors influencing the battlefield. In May 2000, the Joint Chiefs of Staff published Joint Publication (JP) 2-01.3. Entitled "*Joint Tactics, Techniques and Procedures for Intelligence Preparation of the Battlespace,"* or JIPB. The JIPB process extended the Army's traditional IPB methodology into the realms of the electromagnetic spectrum, outer space and the information environment. This new approach was intended to facilitate military operations in the Information Age and to support full-spectrum Information Operations (IO) as discussed in JP 3-13, *Joint Doctrine for Information Operations.*

In cooperation with DARPA and AFRL, ZelTech has taken the next step with JIPB by focusing the process on computer network operations (CNO). This process is called Intelligence Preparation of the Information Battlespace (IPIB). It enables joint force commanders to visualize the entire spectrum of adversary capabilities in every physical and electronic realm where military operations occur today. The IPIB process is used to assist with the production of intelligence estimates, assessments, and other products to support a commander's decision-making process. It is a continuous process involving five steps that help a commander know *where to look* in the battlespace, *when to look*, *what to expect, and what to do to defend the battlespace:*

a. Define the battlespace environment

b. Describe the battlespace's effects

c. Evaluate the threat

d. Determine the threat's potential courses of action (COAs)

e. Apply IPIB through a Cyber Defense or Cyber Attack Plan

By extending the JIPB methodology from kinetic warfare into the cyber realm, analysts may plan CNO using a standardized process. Since cyber attacks operate on a nanosecond timeline, it is crucial for commanders to anticipate an attack and establish countermeasures before the attack takes place. The resulting IPIB products offer commanders an opportunity to conduct cyberspace defense in a proactive vice reactive manner. IPIB is an inherently joint process that can benefit commanders at all levels. It requires close cooperation between a commander's intelligence, operations, and communications staffs.

The IPIB methodology and tools support Network Information Operations (IO) across the full range of military operations from the strategic to the tactical level. The IPIB process can be expanded to provide defensive IO analysis for not only computer networks, but also for the supporting critical infrastructure and human factors comprising the Department of Defense's critical information systems. ZelTech has developed an IPIB software prototype, written in pure Java code. A discussion of the technical aspects of the IPIB program prior to commencement of this task can be found in the Final Technical Report for AFRL Contract F30602-99-C-0168, the initial contract for the IPIB R&D.

3.0 Discussion.

Effort under this task involved three areas of concentration – increased functionality of the IPIB prototype itself, feasibility analyses, and experiment and demonstrations, including modeling and scenario development. Also, due to time constraints and coordination difficulties, three subtasks were deferred to a subsequent effort, which AFRL has recently funded through a separate effort. Each is discussed below:

3.1 IPIB Prototype Enhancements.

The enhancements described herein are those made to the IPIB/CNOAT baseline discussed in paragraph 2.a. First, we merged the two baselines by reincorporating and reintegrating the CNOAT subsystem into IPIB. This gives IPIB a more detailed capability in IPIB Step 2, in that it now produces new products and includes new capabilities – a Master Protection List, which is a list of critical network assets that should be protected (such as ensuring they are first for installation of patches); a Vulnerable Assets list, which is a list of network nodes that are vulnerable to known exploits in the exploits database; a Critical Assets List, which includes assets with direct and implied criticality as described in the Experiments and Demonstrations section below under Measures of Effectiveness; and two discovery tools – a network discovery tool and a software discovery tool for automatically populating their respective databases. This assured that IPIB has the same DIW capabilities as CNOAT. Next, we reactivated the

map capability, and linked it to the IPIB database system so that network sites could be represented both on a map display and in viewable text fields from a data record. The underlying Geographic Information System software is BBN's OpenMap, which is common to the web-based Timeline Analysis System (WebTAS) that is used for map displays and situational awareness visualization in other AFRL initiatives, and is the target GIS for adding and execution-time capability to IPIB in a subsequent effort. There remains one map interaction capability to be done – representation of polygons for classical IPB Areas of Responsibility and Areas of Interest. We also reintegrated the IPIB Attack Tree (AT) capability, which wraps the Commercial-off-the-Shelf (COTS) product SecurITree™ from Amenaza Technologies, Ltd, and extends the ATs to include information necessary for planning and execution support, such as Observables and Countermeasures. We included data fields for linking the AT attributes to the remainder of the IPIB database, but did not accomplish the actual connection under this funding. The final capability added under this task is COA extraction from Attack Trees (AT). IPIB can now extract all the unique COAs from an AT, and display them in a COA array that can be sorted by user-defined metrics. This capability makes IPIB fully useful and suitable for fielding or technology transition into an operational system at a Joint Intelligence Center or Joint Analysis Center, or similar organization that is tasked to produce predictive intelligence about enemy COAs or to generate potential COAs for CNA.

Development of two desired capabilities has been deferred to a subsequent task due to time and resource constraints – interoperability with the Air Force Enterprise Defense (AFED) system, and an early proof-of-concept Cyber Defense Planning capability. We have the Concept of Operation for passing high-threat attacks from IPIB to AFED for detection and correlation, receiving alerts from AFED when a correlated event is detected, and alerting the operator that certain enemy COAs may be in play, including the sequence of expected events in those COAs, but no interface code has been developed. The basic Cyber Defense Planner would take advantage of the stored Observable and Countermeasure attributes at each AT node object to generate defense plans based on predicted most dangerous and/or most likely COAs, including some proactive capability to modify the cyber playbook on the fly in response to observed events. We are implementing these two capabilities under a subsequent effort.

3.2 Feasibility Analyses.

The main feasibility analysis was to determine the feasibility of integrating IPIB with the Topological Vulnerability Analysis (TVA) tool, Combinatorial Analysis Utilizing Logical Dependencies Residing on Networks (CAULDRON), developed by the George Mason University's Center for Secure Information Systems (CSIS). ZelTech and CSIS jointly analyzed two components of feasibility – technical and economic. On the technical side, the concept was that CAULDRON could significantly reduce the manual effort involved in populating the lower levels of IPIB Attack Trees. We developed an interoperability architecture for passing CAULDRON the information it required for TVA – the network architecture, a goal or goals, and a stored suite of exploits and

vulnerabilities. IPIB could use its network description or discovery tool to collect the network architecture model, and, by building IPIB Attack Tree (AT), one could pass selected LEAF nodes to CAULDRON as goals for TVA. An AT is a representation of a hierarchy of strategy-to-task tasks, decomposed to a level suitable for passing an objective to CAULDRON. The concept was that an IPIB user could develop attack trees to a level where a LEAF node represented a goal that one could assign to a competent Red Team or Special Technical Operations (STO) cell and reasonably expect that they could do the further decomposition to execute it. If we could define a common representation of those LEAF goals, then they could be passed to CAULDRON and it would do the further refinement. The CAULDRON products of interest to IPIB are an attack graph represented in XML that could be post processed back into an Attack Subtree expansion of the LEAF node, and a graphic visualization of it for user/analyst display. For the feasibility analysis, we examined the data structures required by CAULDRON and the data available in IPIB, and vice versa for the CAULDRON products. We concluded that it is indeed technically feasible to integrate or interoperated IPIB and CAULDRON. It is economically feasible in that virtually no changes are required in the TVA engine itself, but mainly in data transmission and reception scripts, and a simple executive that directs the receipt of information from IPIB, runs CAULDRON the required number of times for the number of goals that were sent it, and passes the products back to IPIB. For IPIB, the main effort would consist of slight modifications to XML file formats once they are generated, or to the product generation code itself, and new modules for receiving the two attack graph product types and displaying them and/or re-incorporating them into the overall AT (replacing the LEAF nodes with AG subtrees). The labor required would be relatively small, and since neither IPIB nor CAULDRON require large hosts or servers (both can run on desktops or enhanced Windows or Mac laptops), interoperability is clearly technically and economically feasible. As a result, ZelTech has been tasked by AFRL/IFGB to lead an effort to actually perform the integration in a follow-on effort, which is currently underway.

The other feasibility analysis was to have been to examine the Prediction Systems, Inc. network defense Modeling and Simulation (M&S) tool, Defensive Information Operations Planning Tool (DIOPT), for interoperability with IPIB. Prediction Systems personnel were never available for technical interchanges, so, even though a M&S capability available to an IPIB analyst would be a powerful adjunct for testing strategies against COAs, and aiding Effects-based Assessment, we have deferred this study to a subsequent task.

3.3 Experiments and Demonstrations.

For this task, we developed and extended two scenarios, one for network defense and one for network attack. For CND, we instantiated a notional Air Operations Center (AOC) Theater Battle Management Core Systems (TBMCS) system, consisting of an AOC network with subnets for the Plans, Combat Operations, Intelligence, and Core

cells. We used IPIB to load the Mission, Organization, Network Architecture, Vulnerabilities and Exploits databases, and used them to develop ATs for an adversary attempting various Effects-based network attacks on the AOC mission. We then developed proposed defenses for the most likely and most dangerous attacks.

For EBO-based CNA, we inverted the process and prepared a scenario for disrupting or denying the use of an enemy Air Defense System (ADS) solely through network attacks. For this, we had to model an enemy ADS organization, mission/functions, and distributed network that covered fixed and mobile radar sites, headquarters and remote command posts, and missile or AD artillery batteries and the overall communications network connecting these components. The intent was to demonstrate interoperability with the Effects-based Operations Workstation (EBOWS) in Joint Expeditionary Force Experiment (JEFX) 04. Our model included passing selected high-threat cyber Courses of Action (COA) to the EBOWS Strategy Development Tool (SDT) subsystem for comparison or integration of CNA with traditional kinetic warfare methods of assuring air superiority by denying the use of the enemy ADS. However, JEFX 04 participation required separate funding, which did not materialize. We do have an EBO scenario for denying an ADS with nothing but cyber attacks which has been used successfully in numerous technology transition briefings and demonstrations, including papers at Phoenix Challenge conferences.

For the EBO scenarios, we developed Measures of Effectiveness (MOE) metrics for evaluating each goal or sub goal node in the overall AT[1]. Since we express a COA as a path from LEAF to ROOT in the AT, the representation is the same for an AT that includes all modeled COAs, or an individual COA. The ability to extract and sort COAs described above meant that we could use MOEs of Criticality, Lethality, Invisibility, Feasibility, Likelihood, and Risk to evaluate and select the most appropriate COAs for the given scenario. All metrics are scaled from 0 to 1 where a value of 1 is good for the attacker, and a value of 0 is good for the defender. Criticality is a direct user input, or can be derived from the network architecture where a network node contains subcomponents that are critical (e.g., a software application designated as mission critical on a particular host) or directly affected by a connected node that is critical. Lethality is a direct input, assessed by the user or analyst, to measure the effect a successful attack at that level in the AT would have on the mission the network is supporting. Invisibility is a direct input, and represents the degree which the attack, exploit, or sub goal is subject to premature detection. Feasibility is a measure of cost (i.e., 1 – Cost), where Cost measures the technical capability and the resource cost of achieving that particular attack sub goal. Likelihood is a weighted sum of Lethality, Invisibility, and Feasibility, where the weights are assigned by expectations of adversary goals by adversary type. For instance, a criminal or spy may place a high weight on Invisibility, and a low weight on Lethality, while a terrorist might place a high weight on Lethality, and a high weight on Invisibility until a certain goal is reached, then use a low weight when the "packet of death" is launched and he wants the attack detected. The weighted sums are normalized

[1] Both the SecurITree and IPIB applications calculate the value of the entire tree by rolling up values from child nodes to the parent or pushing down values from a parent to its children. This is the key to creating sortable COAs where the resultant aggregated metrics are displayed and used as sort criteria.

so the Likelihood range remains 0-1. Risk is the traditional definition, Likelihood x Criticality. The user can sort the complete list of COAs by any one metric or any combination in any order of precedence to arrive at a subset of the most dangerous, most likely, cheapest, or most appropriate according to his situation-dependent definition of appropriateness. Thus, we have a first cut at MOEs for EBO. We do not have a means of comparing MOEs for cyber attacks with MOEs for kinetic attacks, since we expected the SDT to be able to do that when IPIB passed a selected (recommended) set of COAs to SDT for inclusion with kinetic attacks.

Under contract funds for this Task, we conducted demonstrations at ZelTech and at the AFRL/IFGB laboratory. We also conducted numerous demonstrations at U&S Commands, other laboratories, and other AF Centers using ZelTech's own business development funds in an effort to generate other technology transition advocacy.

4.0 Conclusions.

See the IPIB Final Technical Report for F30602-99-C-0168.

5.0 Future Research Topics.

See above and the IPIB Final Technical Report for F30602-99-C-0168.

6.0 Points of Contact.

a. Dr. James K. Williams, Principal Investigator, (757) 722-5565, kwilliams@zeltech.com. .

b. Mr. Darich Runyan, Senior Information Security Engineer, (757) 722-5565, darich.runyan@zeltech.com.